Chapter 18: Cosets

Let H be a subgroup of G. For $a, b \in G$ define

$$a \sim_H b \iff a^{-1}b \in H$$
$$\iff$$
$$\iff$$

$\sim_H$ is an equivalence relation on G:

reflexive:

symmetric:

transitive:

For $a \in G$, the equivalence class $[a]$ is:

$$[a] = \{ b \in G \mid a \sim_H b \}$$
$$= \{ b \in G \mid$$
$$=$$
$$=$$

We call $aH = \{ ah \mid h \in H \}$ the <u>left coset</u> of H containing a.

(Similarly, $Ha = \{ ha \mid h \in H \}$ is a <u>right coset</u>. These are the equivalence classes of

$$a \sim b \iff ab^{-1} \in H \text{)}$$

Examples:

① $S_3 = \{ \varepsilon, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2) \}$

$H = \langle (2\,3) \rangle = \{ \varepsilon, (2\,3) \}$

Cosets:

$H =$

Find the right cosets and a set of representatives.

(con't)

$K = \langle(123)\rangle = \{\varepsilon, (123), (132)\} \leq S_3$

Left cosets of K:

$K =$

② $\mathbb{Z}_{16} = \{0,1,2,3,\dots,13,14,15\}$ under $+$, addition modulo 16.

$H = \langle 4\rangle = \{0,4,8,12\}$

Left Cosets of H in $\mathbb{Z}_{16}$:

Lemma 18.1.2 — Properties of Cosets. Let H be a subgroup of G and $a \in G$.

(a) $a \in aH$

(b) $aH = H \iff a \in H$

(c) For $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$.

(d) $aH = bH \iff a^{-1}b \in H \iff b^{-1}a \in H$

(e) If H is finite then $|aH| = |H|$

(f) $aH = Ha \iff a^{-1}Ha = H$.

(Note that by $a^{-1}Ha$ we mean the set $\{a^{-1}ha \mid h \in H\}$.)

Proof: $\sim_H$ is an equivalence relation and $[a] = aH$ are the equivalence classes. Therefore, Lemma 17.1 implies (a), (d), (c). Part (b) is a special case of (d). All that remains to prove is (e) and (f).

(e)

Lagrange's Theorem :

Theorem 18.2.1 — Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Proof :

$\square$

It follows that ,

$$[\text{\# of distinct left cosets}] = |G|/|H| \qquad (= \text{\# distinct right cosets})$$

This number is called the <u>index</u> of H in G :

$$[G:H] = |G|/|H|$$

Corollary 18.2.2 — $ord(a)$ divides $|G|$. Let G be a finite group and $a \in G$. Then

(a) $ord(a)$ divides $|G|$.

(b) $a^{|G|} = e$.